Fig.1

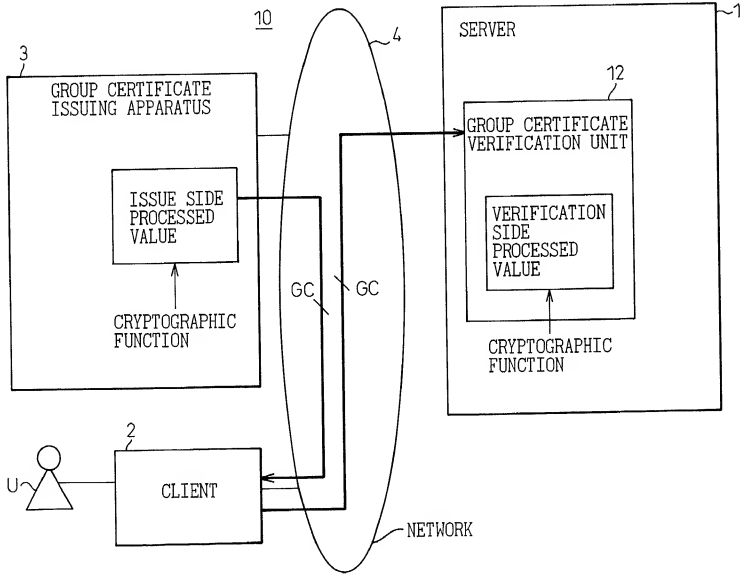

10
4
SERVER
1
3
12
GROUP CERTIFICATE ISSUING APPARATUS
GROUP CERTIFICATE VERIFICATION UNIT
ISSUE SIDE PROCESSED VALUE
VERIFICATION SIDE PROCESSED VALUE
GC
GC
CRYPTOGRAPHIC FUNCTION
CRYPTOGRAPHIC FUNCTION
2
U
CLIENT
NETWORK

Fig.2

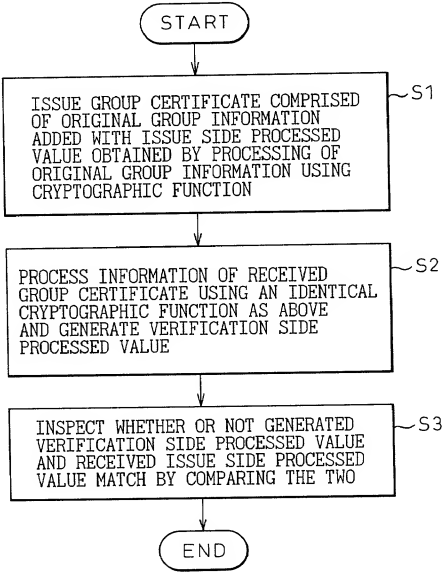

START
ISSUE GROUP CERTIFICATE COMPRISED OF ORIGINAL GROUP INFORMATION ADDED WITH ISSUE SIDE PROCESSED VALUE OBTAINED BY PROCESSING OF ORIGINAL GROUP INFORMATION USING CRYPTOGRAPHIC FUNCTION
S1
PROCESS INFORMATION OF RECEIVED GROUP CERTIFICATE USING AN IDENTICAL CRYPTOGRAPHIC FUNCTION AS ABOVE AND GENERATE VERIFICATION SIDE PROCESSED VALUE
S2
INSPECT WHETHER OR NOT GENERATED VERIFICATION SIDE PROCESSED VALUE AND RECEIVED ISSUE SIDE PROCESSED VALUE MATCH BY COMPARING THE TWO
S3
END

Fig.3

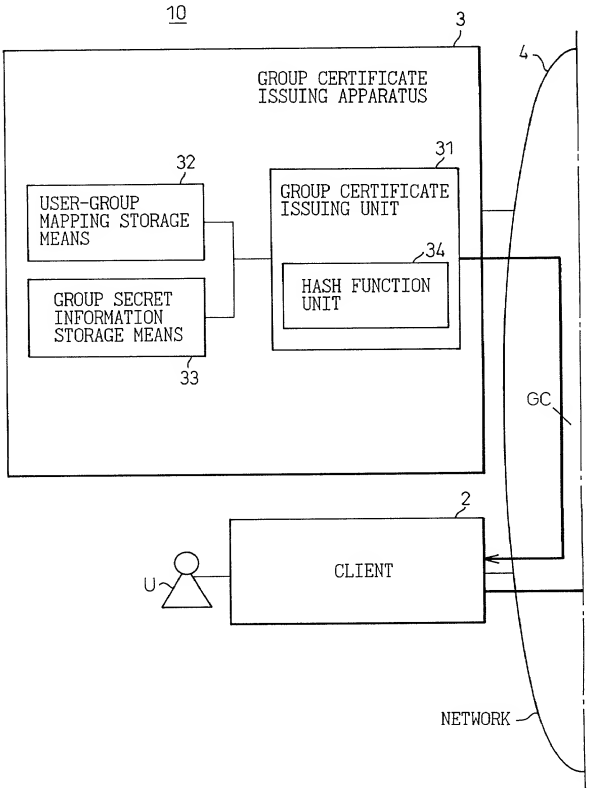

10
3
4
GROUP CERTIFICATE ISSUING APPARATUS
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GC
2
CLIENT
U
NETWORK

Fig. 4

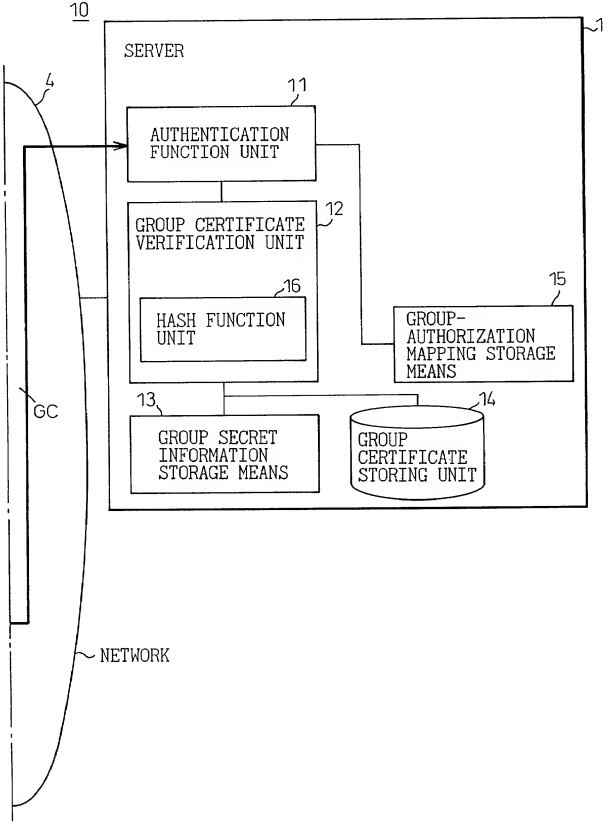

10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
12
GROUP CERTIFICATE VERIFICATION UNIT
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
13
GROUP SECRET INFORMATION STORAGE MEANS
14
GROUP CERTIFICATE STORING UNIT
GC
NETWORK

Fig.5

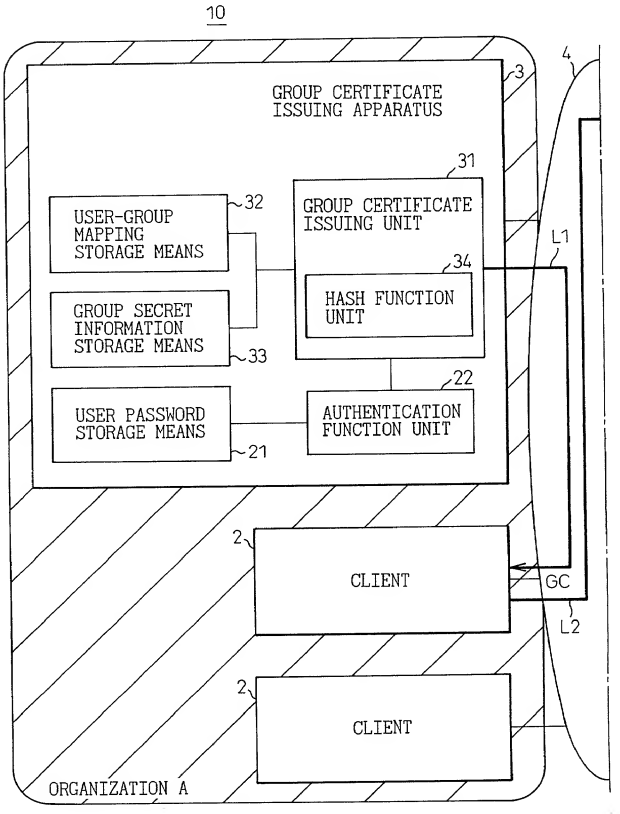

10
GROUP CERTIFICATE ISSUING APPARATUS
3
4
31
USER-GROUP MAPPING STORAGE MEANS
32
GROUP CERTIFICATE ISSUING UNIT
L1
34
HASH FUNCTION UNIT
GROUP SECRET INFORMATION STORAGE MEANS
33
22
USER PASSWORD STORAGE MEANS
21
AUTHENTICATION FUNCTION UNIT
2
CLIENT
GC
L2
2
CLIENT
ORGANIZATION A

Fig.6

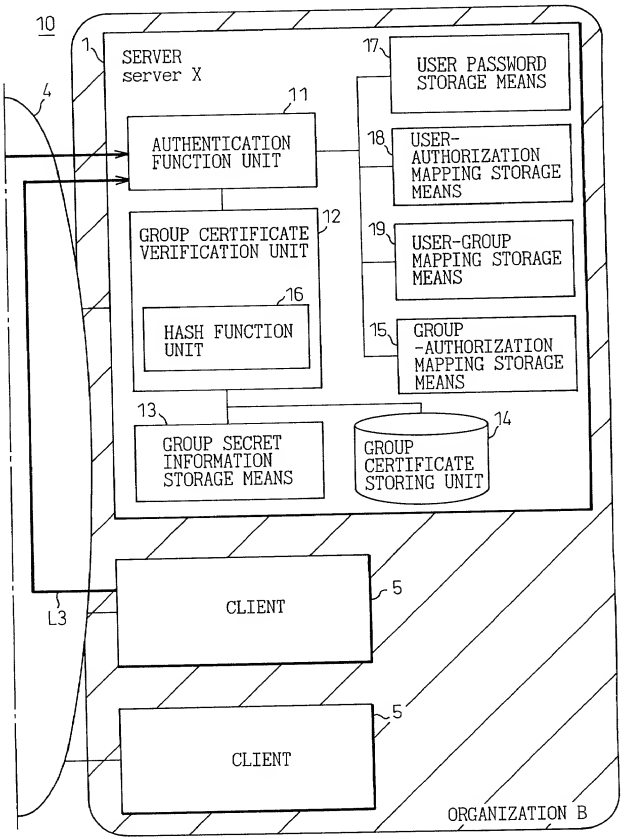

10
1
SERVER
server X
4
11
AUTHENTICATION FUNCTION UNIT
12
GROUP CERTIFICATE VERIFICATION UNIT
16
HASH FUNCTION UNIT
13
GROUP SECRET INFORMATION STORAGE MEANS
14
GROUP CERTIFICATE STORING UNIT
17
USER PASSWORD STORAGE MEANS
18
USER-AUTHORIZATION MAPPING STORAGE MEANS
19
USER-GROUP MAPPING STORAGE MEANS
15
GROUP -AUTHORIZATION MAPPING STORAGE MEANS
L3
CLIENT
5
CLIENT
5
ORGANIZATION B

Fig. 7

USER	GROUP
server X,user A server X,user B server Y,user A server Y,user C ⋮	server X.group 3 server X.group 1 server Y.group 4 server Y.group 4 ⋮

Fig. 8

USER	GROUP
server X,user A server X,user B server Y,user A server Y,user C ⋮	server X.group 3 server X.group 1 server Y.group 4 server Y.group 4 ⋮

Fig.9

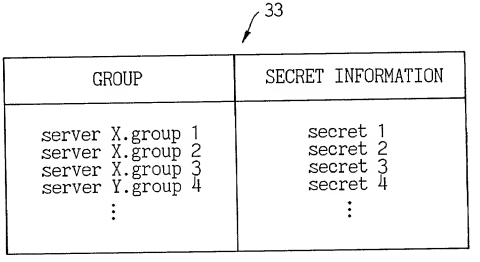

33
GROUP
SECRET INFORMATION
server X.group 1
server X.group 2
server X.group 3
server Y.group 4
secret 1
secret 2
secret 3
secret 4

Fig.10

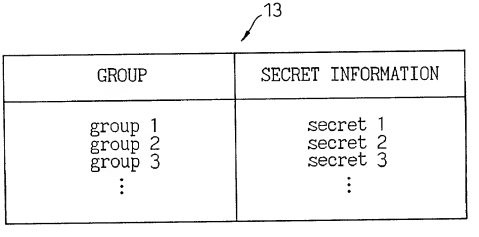
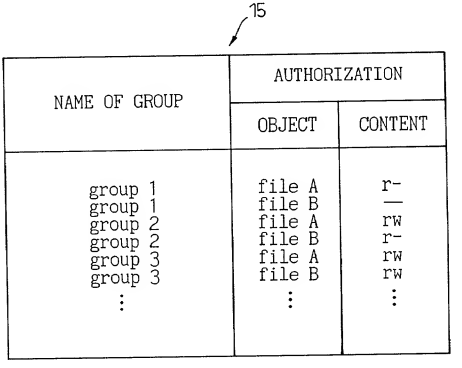

13
GROUP
SECRET INFORMATION
group 1
group 2
group 3
secret 1
secret 2
secret 3

Fig.11


15
NAME OF GROUP
AUTHORIZATION
OBJECT
CONTENT
group 1
group 1
group 2
group 2
group 3
group 3
file A
file B
file A
file B
file A
file B
r-
—
rw
r-
rw
rw

PCT/JP2003/000000

Fig.12

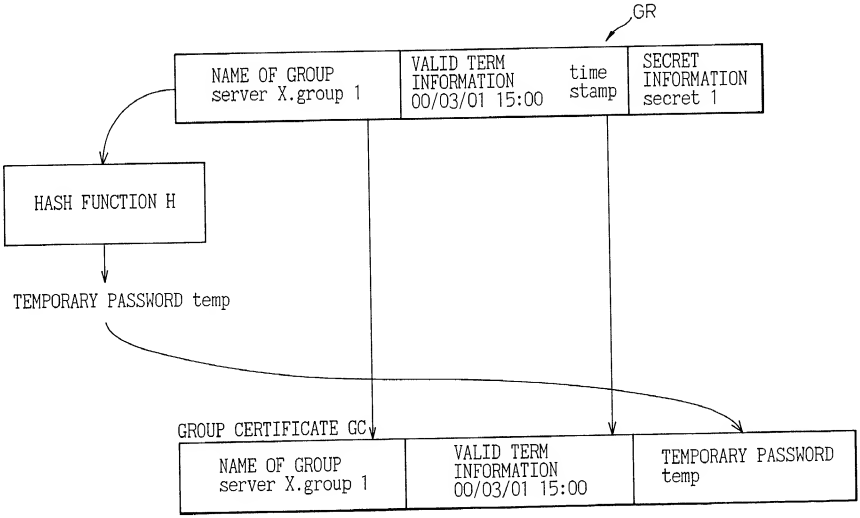


Fig. 13

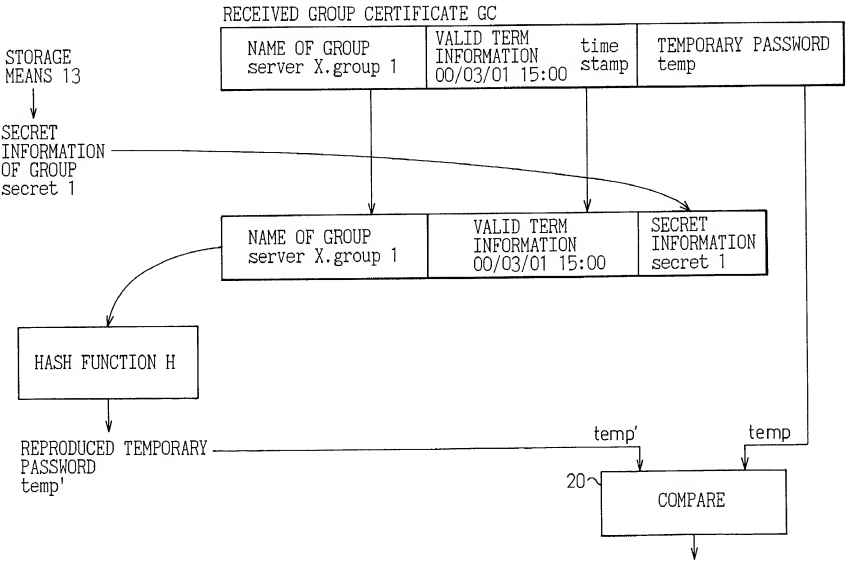

RECEIVED GROUP CERTIFICATE GC
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
time stamp
TEMPORARY PASSWORD temp
STORAGE MEANS 13
SECRET INFORMATION OF GROUP secret 1
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
SECRET INFORMATION secret 1
HASH FUNCTION H
REPRODUCED TEMPORARY PASSWORD temp'
temp'
temp
20
COMPARE

Fig.14

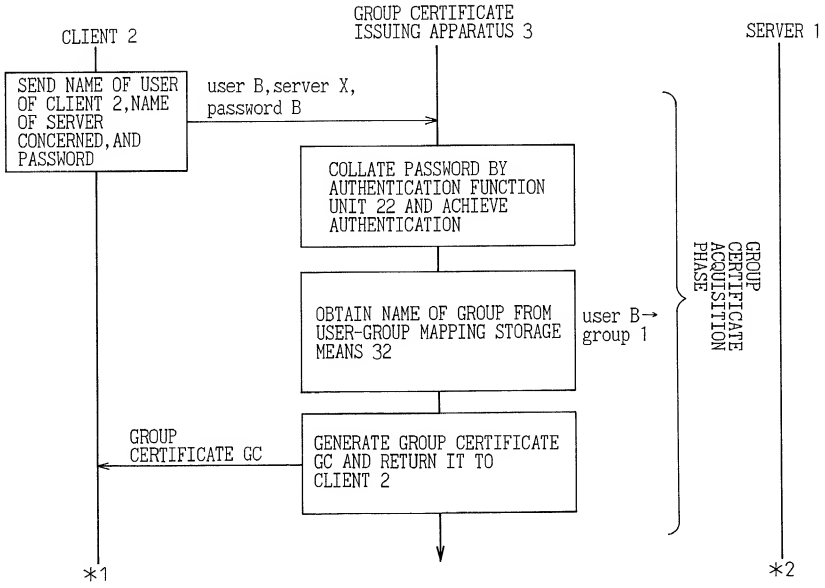

CLIENT 2
GROUP CERTIFICATE ISSUING APPARATUS 3
SERVER 1
SEND NAME OF USER OF CLIENT 2, NAME OF SERVER CONCERNED, AND PASSWORD
user B, server X, password B
COLLATE PASSWORD BY AUTHENTICATION FUNCTION UNIT 22 AND ACHIEVE AUTHENTICATION
OBTAIN NAME OF GROUP FROM USER-GROUP MAPPING STORAGE MEANS 32
user B→ group 1
GENERATE GROUP CERTIFICATE GC AND RETURN IT TO CLIENT 2
GROUP CERTIFICATE GC
GROUP CERTIFICATE ACQUISITION PHASE
*1
*2

Fig.15

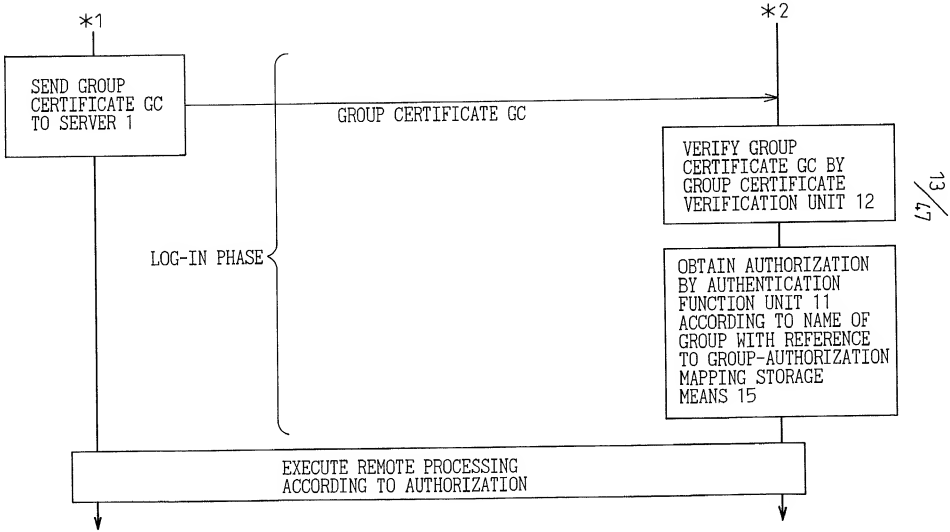

*1
*2
SEND GROUP CERTIFICATE GC TO SERVER 1
GROUP CERTIFICATE GC
VERIFY GROUP CERTIFICATE GC BY GROUP CERTIFICATE VERIFICATION UNIT 12
LOG-IN PHASE
OBTAIN AUTHORIZATION BY AUTHENTICATION FUNCTION UNIT 11 ACCORDING TO NAME OF GROUP WITH REFERENCE TO GROUP-AUTHORIZATION MAPPING STORAGE MEANS 15
EXECUTE REMOTE PROCESSING ACCORDING TO AUTHORIZATION

Fig.16

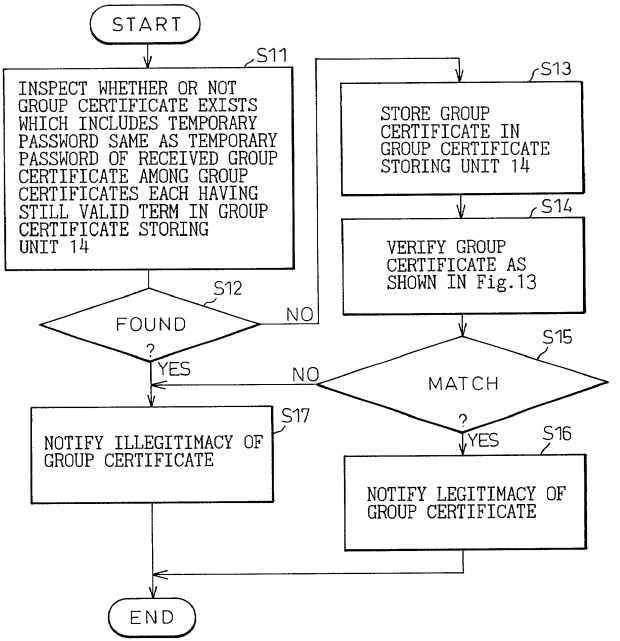

START
S11
INSPECT WHETHER OR NOT GROUP CERTIFICATE EXISTS WHICH INCLUDES TEMPORARY PASSWORD SAME AS TEMPORARY PASSWORD OF RECEIVED GROUP CERTIFICATE AMONG GROUP CERTIFICATES EACH HAVING STILL VALID TERM IN GROUP CERTIFICATE STORING UNIT 14
S12
FOUND ?
NO
YES
S13
STORE GROUP CERTIFICATE IN GROUP CERTIFICATE STORING UNIT 14
S14
VERIFY GROUP CERTIFICATE AS SHOWN IN Fig.13
S15
MATCH ?
NO
YES
S16
NOTIFY LEGITIMACY OF GROUP CERTIFICATE
S17
NOTIFY ILLEGITIMACY OF GROUP CERTIFICATE
END

Fig.17

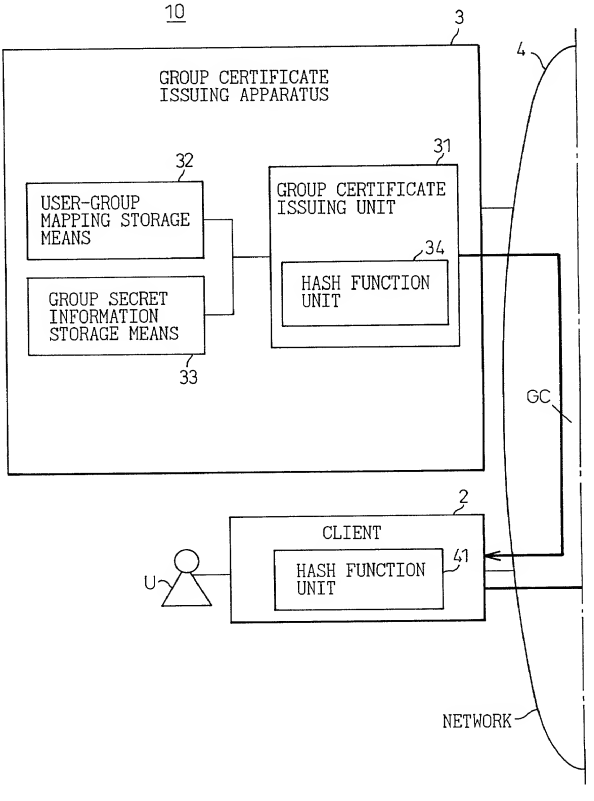

10
3
4
GROUP CERTIFICATE ISSUING APPARATUS
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GC
2
CLIENT
41
HASH FUNCTION UNIT
U
NETWORK

Fig.18

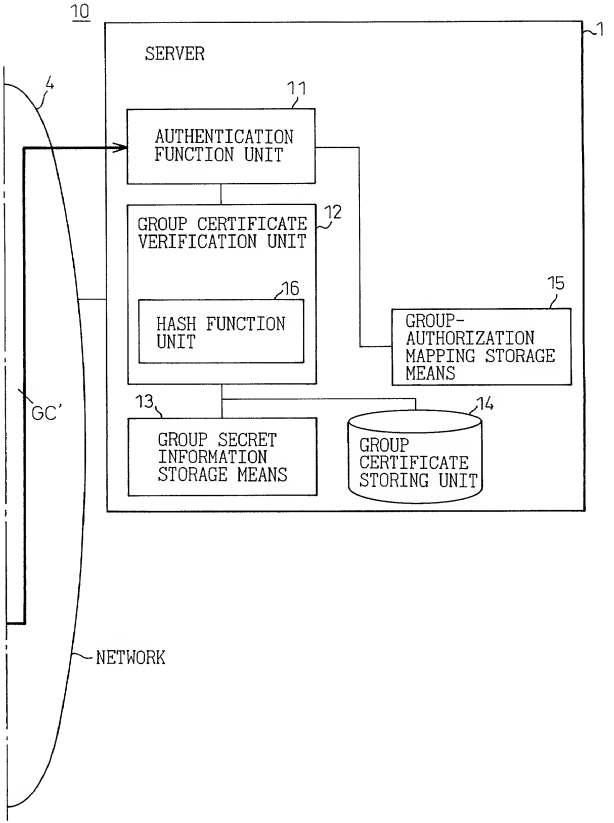

10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
GROUP CERTIFICATE VERIFICATION UNIT
12
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
GC'
13
GROUP SECRET INFORMATION STORAGE MEANS
14
GROUP CERTIFICATE STORING UNIT
NETWORK

Fig.19

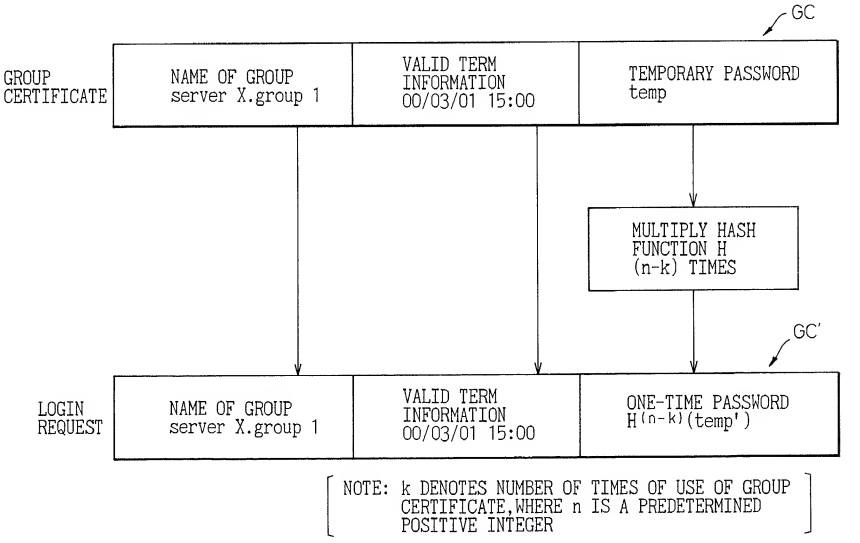

GC
GROUP CERTIFICATE
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
TEMPORARY PASSWORD temp
MULTIPLY HASH FUNCTION H (n-k) TIMES
GC'
LOGIN REQUEST
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
ONE-TIME PASSWORD H(n-k)(temp')
NOTE: k DENOTES NUMBER OF TIMES OF USE OF GROUP CERTIFICATE, WHERE n IS A PREDETERMINED POSITIVE INTEGER

Fig.20

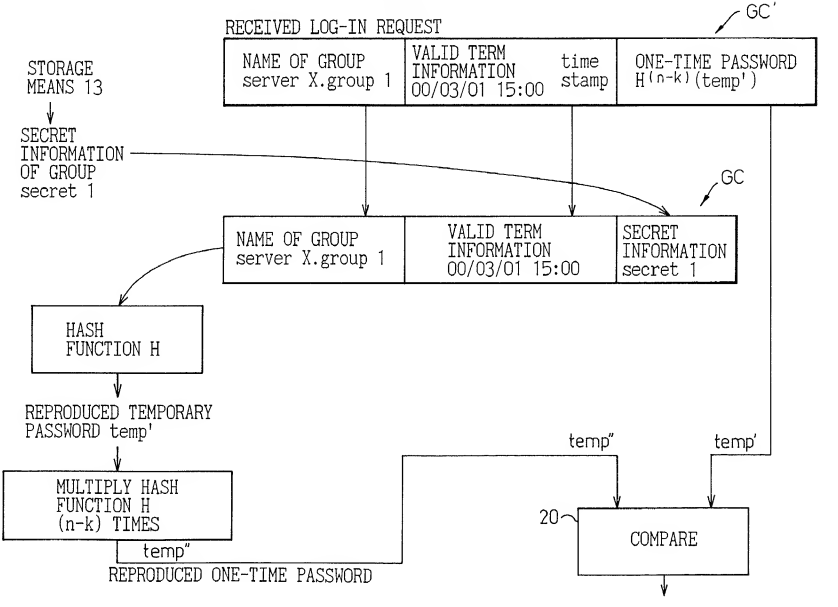

RECEIVED LOG-IN REQUEST
GC'
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
time stamp
ONE-TIME PASSWORD H(n-k)(temp')
STORAGE MEANS 13
SECRET INFORMATION OF GROUP secret 1
GC
NAME OF GROUP server X.group 1
VALID TERM INFORMATION 00/03/01 15:00
SECRET INFORMATION secret 1
HASH FUNCTION H
REPRODUCED TEMPORARY PASSWORD temp'
MULTIPLY HASH FUNCTION H (n-k) TIMES
temp"
REPRODUCED ONE-TIME PASSWORD
temp"
temp'
20
COMPARE

Fig. 21

LOG-IN REQUEST GC'			VALUE OF k
NAME OF GROUP	VALID TERM INFORMATION time stamp	ONE-TIME PASSWORD temp'	
server X.group 1	00/03/01 15:00	$H^{(n)}(temp')$	0
server X.group 4	00/03/01 13:00	$H^{(n-4)}(temp')$	4
server X.group 2	00/03/01 14:00	$H^{(n-6)}(temp')$	6
⋮	⋮	⋮	⋮

Fig. 22

CLIENT 2
GROUP CERTIFICATE ISSUING APPARATUS 3
SERVER 1
GROUP CERTIFICATE ACQUISITION PHASE
SEND NAME OF USER OF CLIENT 2, NAME OF SERVER CONCERNED, AND PASSWORD
user B, server X, password B
CHECK PASSWORD BY AUTHENTICATION FUNCTION UNIT 22 FOR AUTHENTICATION
OBTAIN NAME OF GROUP FROM USER-GROUP MAPPING STORAGE MEANS 32
user B → gruop 1
GENERATE GROUP CERTIFICATE GC AND RETURN IT TO CLIENT 2
GROUP CERTIFICATE GC
*1
*2

Fig. 23

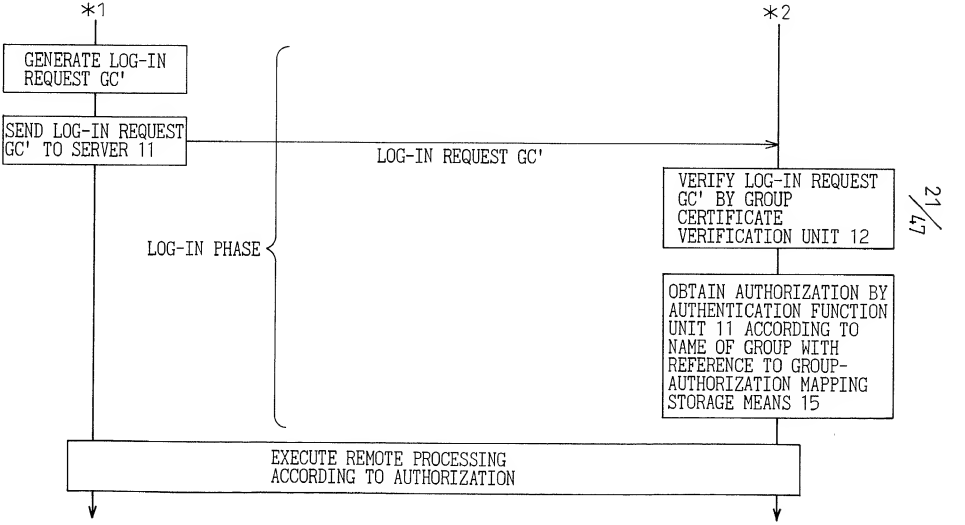

*1
*2
GENERATE LOG-IN REQUEST GC'
SEND LOG-IN REQUEST GC' TO SERVER 11
LOG-IN REQUEST GC'
VERIFY LOG-IN REQUEST GC' BY GROUP CERTIFICATE VERIFICATION UNIT 12
LOG-IN PHASE
OBTAIN AUTHORIZATION BY AUTHENTICATION FUNCTION UNIT 11 ACCORDING TO NAME OF GROUP WITH REFERENCE TO GROUP-AUTHORIZATION MAPPING STORAGE MEANS 15
EXECUTE REMOTE PROCESSING ACCORDING TO AUTHORIZATION

Fig.24

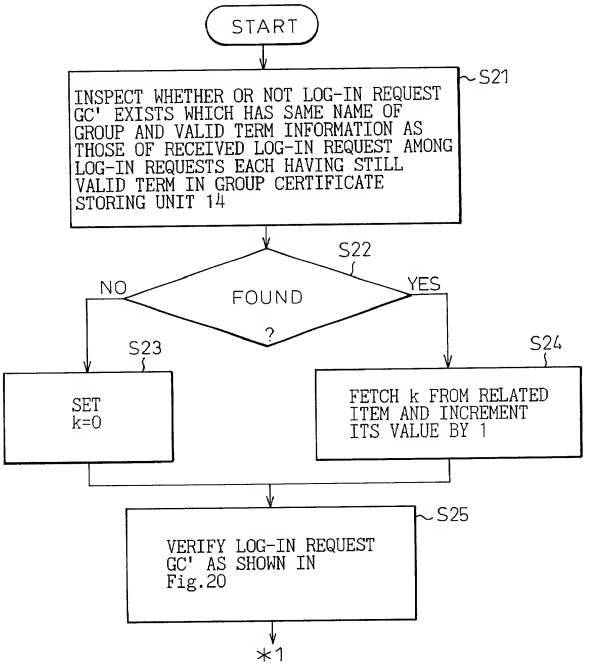

START
INSPECT WHETHER OR NOT LOG-IN REQUEST GC' EXISTS WHICH HAS SAME NAME OF GROUP AND VALID TERM INFORMATION AS THOSE OF RECEIVED LOG-IN REQUEST AMONG LOG-IN REQUESTS EACH HAVING STILL VALID TERM IN GROUP CERTIFICATE STORING UNIT 14
S21
FOUND ?
S22
NO
YES
SET k=0
S23
FETCH k FROM RELATED ITEM AND INCREMENT ITS VALUE BY 1
S24
VERIFY LOG-IN REQUEST GC' AS SHOWN IN Fig.20
S25
*1

Fig.25

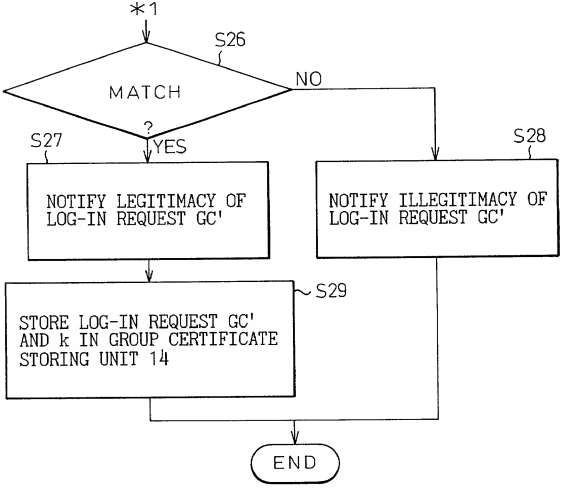

*1
S26
MATCH
?
NO
YES
S27
S28
NOTIFY LEGITIMACY OF LOG-IN REQUEST GC'
NOTIFY ILLEGITIMACY OF LOG-IN REQUEST GC'
S29
STORE LOG-IN REQUEST GC' AND k IN GROUP CERTIFICATE STORING UNIT 14
END

Fig.26

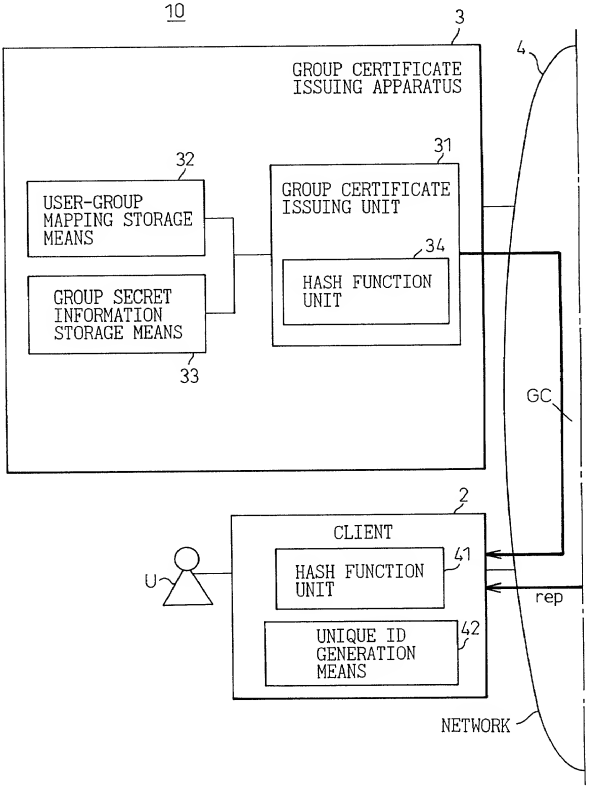
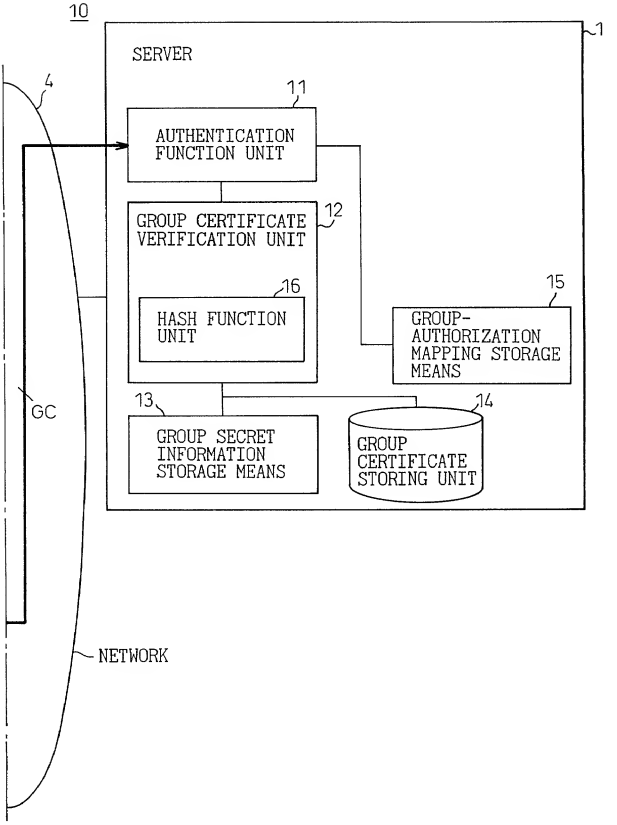

10
3
4
GROUP CERTIFICATE ISSUING APPARATUS
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GC
2
CLIENT
U
HASH FUNCTION UNIT
41
rep
UNIQUE ID GENERATION MEANS
42
NETWORK

Fig.27


10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
GROUP CERTIFICATE VERIFICATION UNIT
12
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
GC
13
14
GROUP SECRET INFORMATION STORAGE MEANS
GROUP CERTIFICATE STORING UNIT
NETWORK

PATENT CABINET

Fig. 28

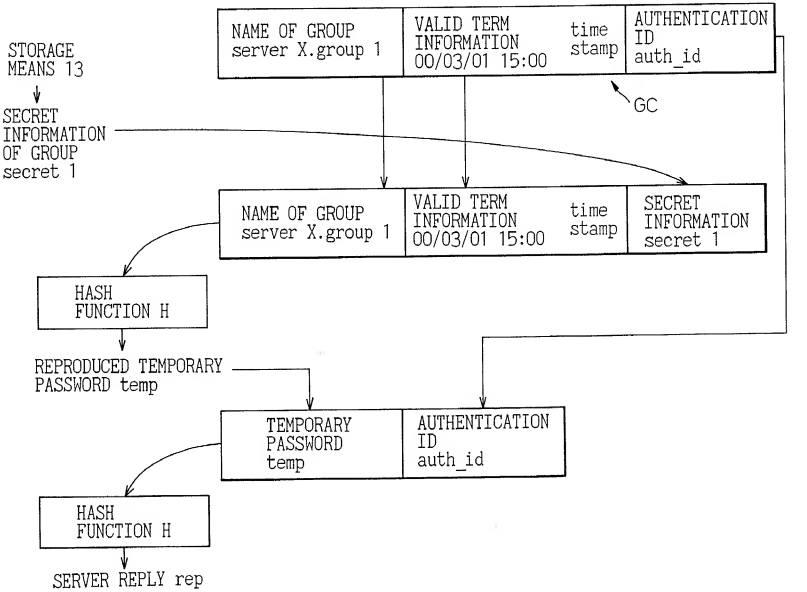


Fig. 29

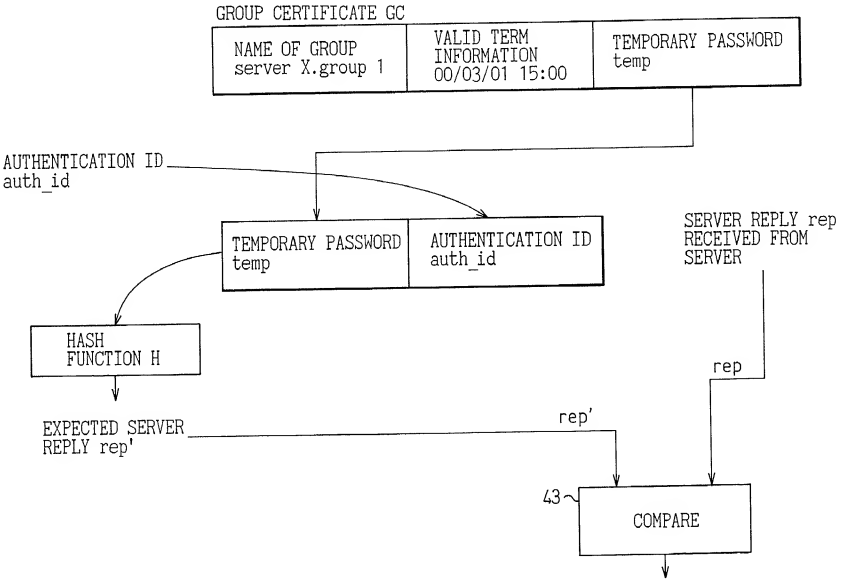

GROUP CERTIFICATE GC
NAME OF GROUP
server X.group 1
VALID TERM INFORMATION
00/03/01 15:00
TEMPORARY PASSWORD
temp
AUTHENTICATION ID
auth_id
TEMPORARY PASSWORD
temp
AUTHENTICATION ID
auth_id
SERVER REPLY rep
RECEIVED FROM
SERVER
HASH
FUNCTION H
rep
EXPECTED SERVER
REPLY rep'
rep'
43
COMPARE

Fig.30

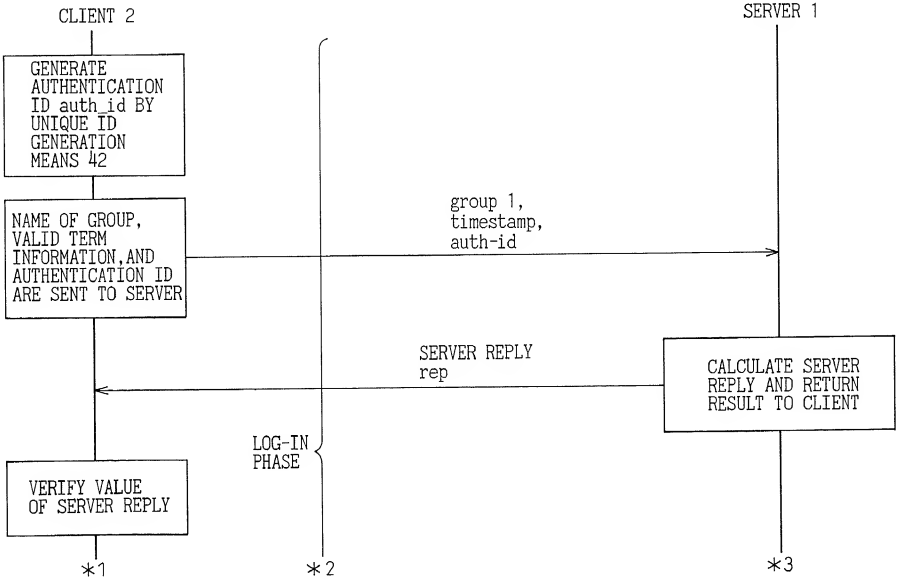

CLIENT 2
SERVER 1
GENERATE AUTHENTICATION ID auth_id BY UNIQUE ID GENERATION MEANS 42
NAME OF GROUP, VALID TERM INFORMATION, AND AUTHENTICATION ID ARE SENT TO SERVER
group 1, timestamp, auth-id
SERVER REPLY rep
CALCULATE SERVER REPLY AND RETURN RESULT TO CLIENT
LOG-IN PHASE
VERIFY VALUE OF SERVER REPLY
*1
*2
*3

Fig.31

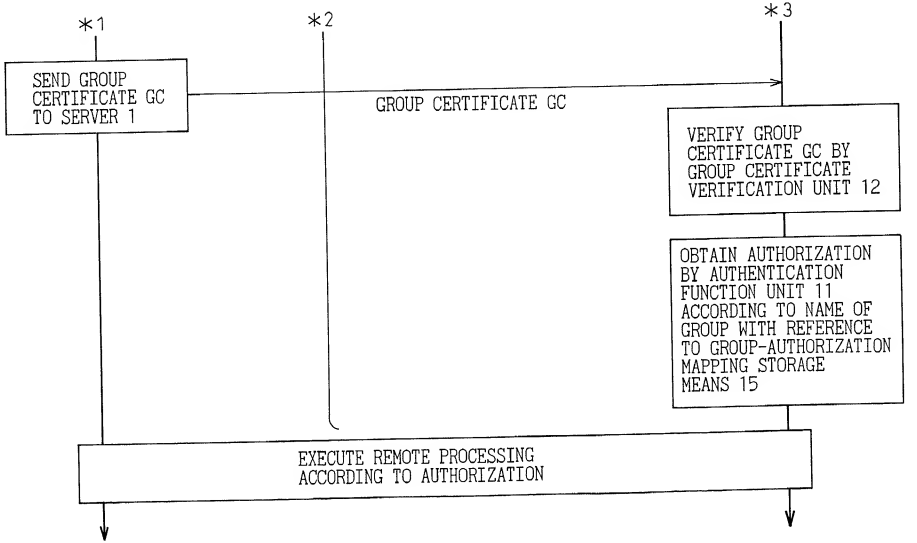

*1
*2
*3
SEND GROUP CERTIFICATE GC TO SERVER 1
GROUP CERTIFICATE GC
VERIFY GROUP CERTIFICATE GC BY GROUP CERTIFICATE VERIFICATION UNIT 12
OBTAIN AUTHORIZATION BY AUTHENTICATION FUNCTION UNIT 11 ACCORDING TO NAME OF GROUP WITH REFERENCE TO GROUP-AUTHORIZATION MAPPING STORAGE MEANS 15
EXECUTE REMOTE PROCESSING ACCORDING TO AUTHORIZATION

Fig. 32

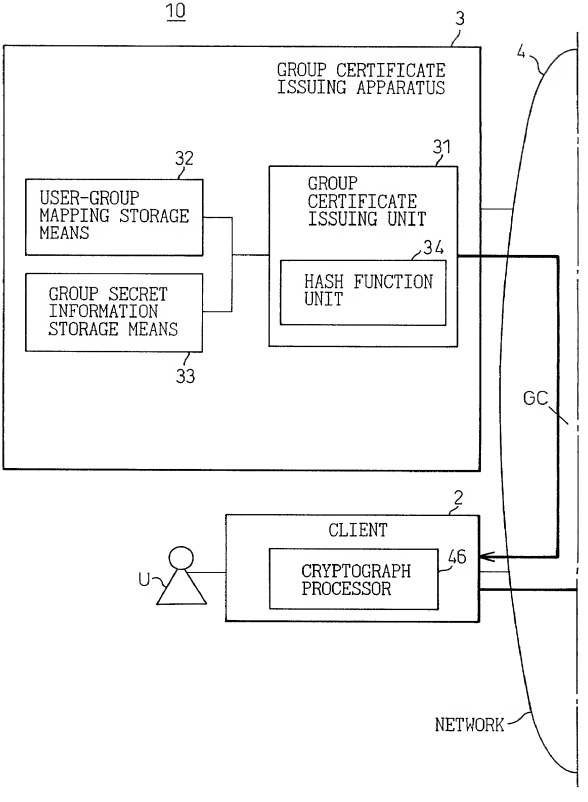

10
3
GROUP CERTIFICATE ISSUING APPARATUS
4
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GC
2
CLIENT
46
CRYPTOGRAPH PROCESSOR
U
NETWORK

Fig.33

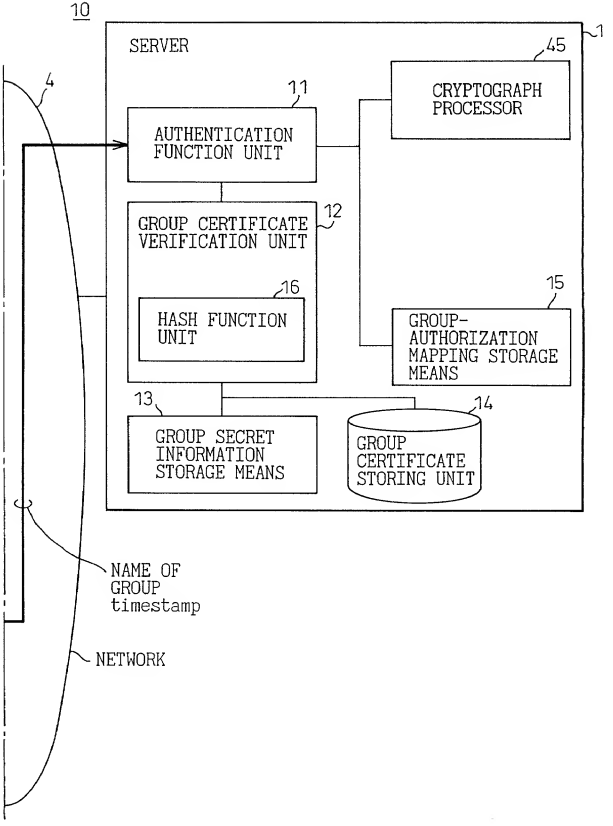

10
SERVER
1
45
CRYPTOGRAPH PROCESSOR
4
11
AUTHENTICATION FUNCTION UNIT
12
GROUP CERTIFICATE VERIFICATION UNIT
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
13
GROUP SECRET INFORMATION STORAGE MEANS
14
GROUP CERTIFICATE STORING UNIT
NAME OF GROUP
timestamp
NETWORK

Fig.34

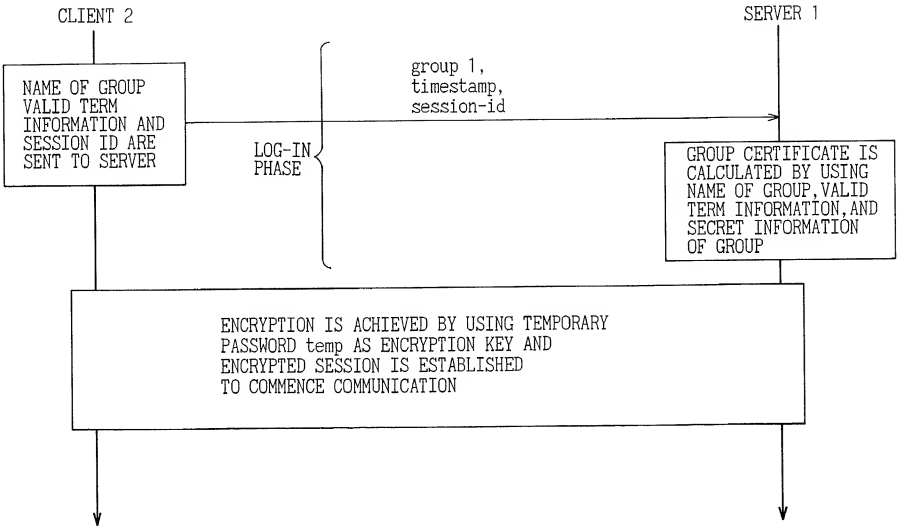

CLIENT 2
SERVER 1
NAME OF GROUP VALID TERM INFORMATION AND SESSION ID ARE SENT TO SERVER
group 1, timestamp, session-id
LOG-IN PHASE
GROUP CERTIFICATE IS CALCULATED BY USING NAME OF GROUP, VALID TERM INFORMATION, AND SECRET INFORMATION OF GROUP
ENCRYPTION IS ACHIEVED BY USING TEMPORARY PASSWORD temp AS ENCRYPTION KEY AND ENCRYPTED SESSION IS ESTABLISHED TO COMMENCE COMMUNICATION

Fig.35

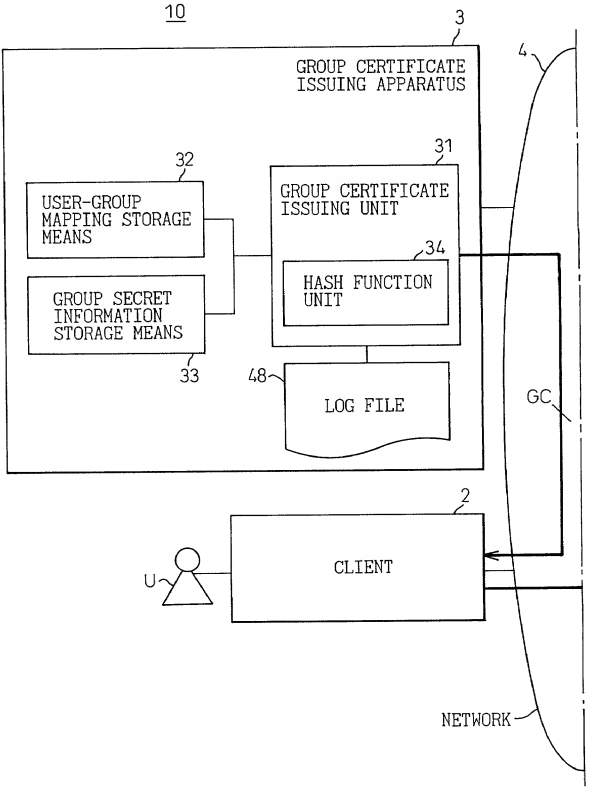
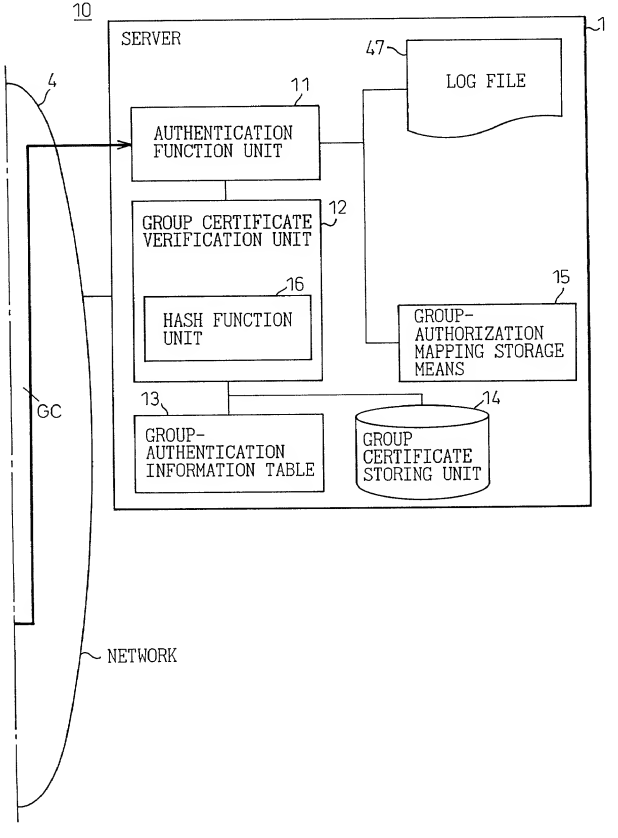

10
3
GROUP CERTIFICATE ISSUING APPARATUS
4
31
32
USER-GROUP MAPPING STORAGE MEANS
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GROUP SECRET INFORMATION STORAGE MEANS
33
48
LOG FILE
GC
2
CLIENT
U
NETWORK

Fig.36


10
SERVER
1
47
LOG FILE
4
11
AUTHENTICATION FUNCTION UNIT
12
GROUP CERTIFICATE VERIFICATION UNIT
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
GC
13
GROUP-AUTHENTICATION INFORMATION TABLE
14
GROUP CERTIFICATE STORING UNIT
NETWORK

EUROPEAN SEARCH REPORT

Fig.37

LOG FILE OF GROUP CERTIFICATE ISSUING APPARATUS

48

ISSUE DATE AND TIME	USER	SERVER	GROUP	VALID TERM INFORMATION	TEMPORARY PASSWORD temp
00/03/01 09:42	user A	server X	group 2	00/03/01 13:00	2983301136
00/03/01 10:25	user B	server X	group 1	00/03/01 15:00	4023502123
⋮	⋮	⋮	⋮	⋮	⋮

Fig. 38

47

LOG FILE OF SERVER

START DATE AND TIME OF PROCESSING	FINISH DATE AND TIME OF PROCESSING	NAME OF CLIENT HOST	GROUP	VALID TERM INFORMATION	TEMPORARY PASSWORD temp
00/03/01 10:14 00/03/01 10:25 ⋮	00/03/01 12:20 00/03/01 14:41 ⋮	host J host K ⋮	group 2 group 1 ⋮	00/03/01 13:00 00/03/01 15:00 ⋮	2983301136 4023502123 ⋮

Fig. 39

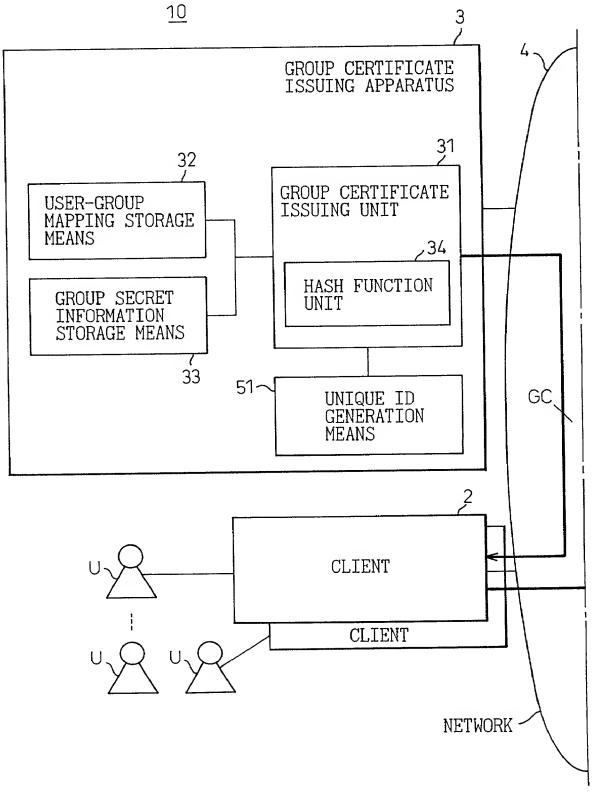
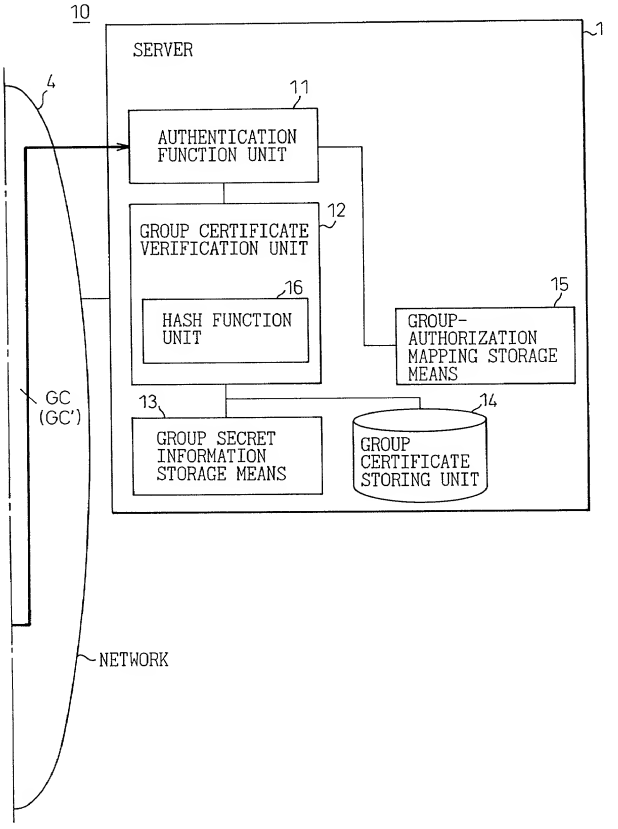

10
3
GROUP CERTIFICATE ISSUING APPARATUS
4
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
51
UNIQUE ID GENERATION MEANS
GC
2
CLIENT
CLIENT
U
U
U
NETWORK

Fig. 40


10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
12
GROUP CERTIFICATE VERIFICATION UNIT
16
HASH FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
GC (GC')
13
GROUP SECRET INFORMATION STORAGE MEANS
14
GROUP CERTIFICATE STORING UNIT
NETWORK

POSTED: 02/26/2004

Fig.41

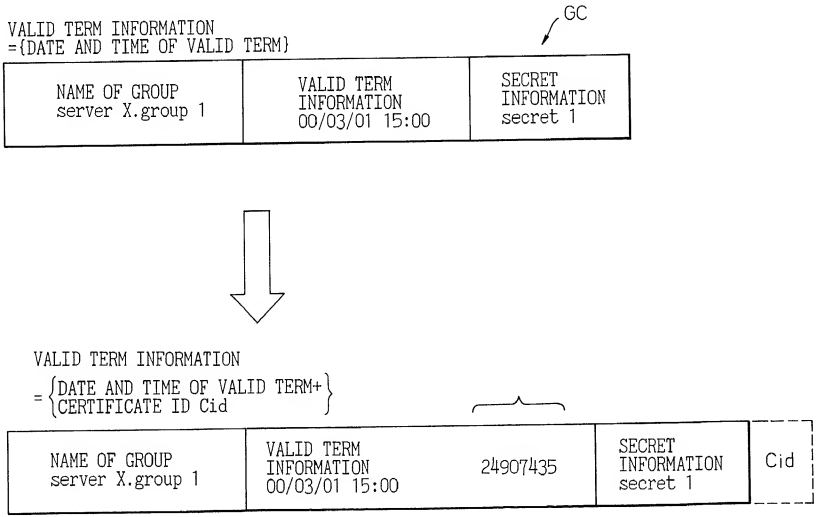


Fig.42

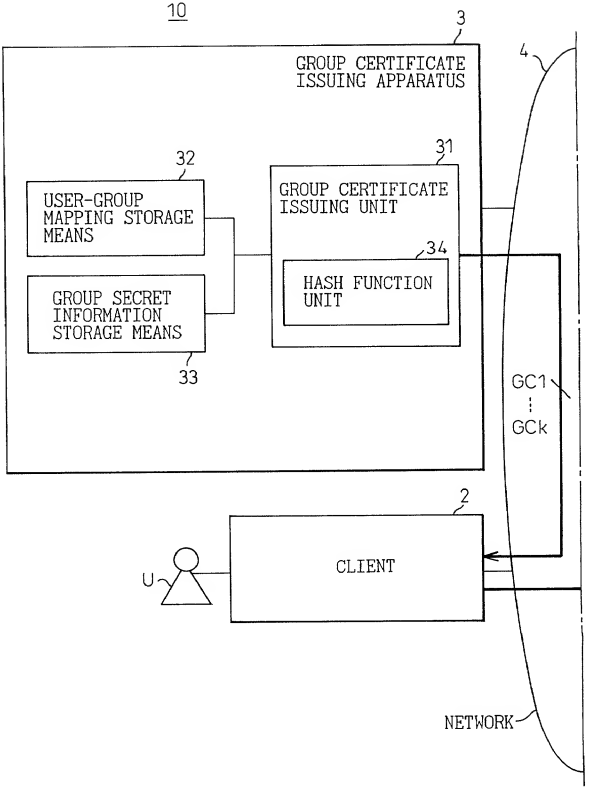

10
3
GROUP CERTIFICATE ISSUING APPARATUS
4
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31
GROUP CERTIFICATE ISSUING UNIT
34
HASH FUNCTION UNIT
GC1
GCk
2
CLIENT
U
NETWORK

Fig. 43

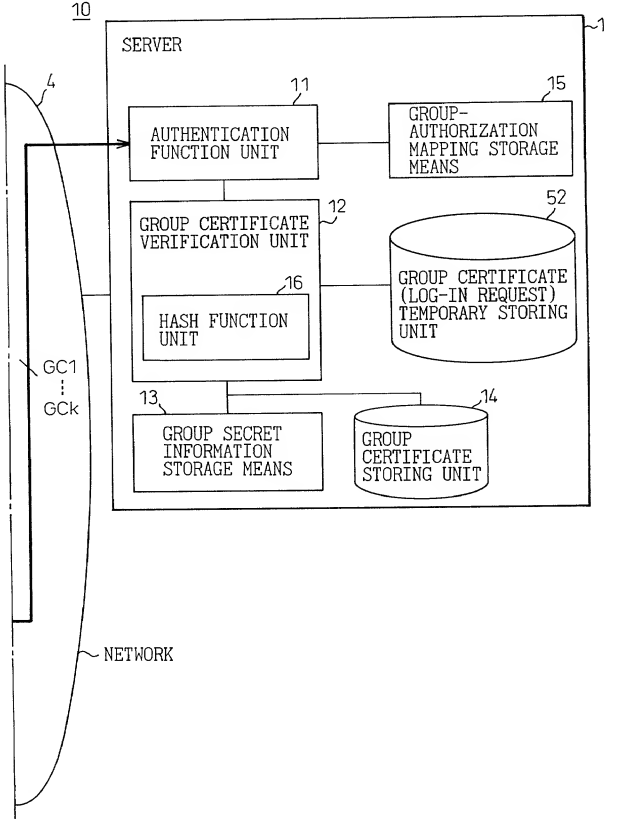

10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
12
GROUP CERTIFICATE VERIFICATION UNIT
52
16
HASH FUNCTION UNIT
GROUP CERTIFICATE (LOG-IN REQUEST) TEMPORARY STORING UNIT
GC1
GCk
13
14
GROUP SECRET INFORMATION STORAGE MEANS
GROUP CERTIFICATE STORING UNIT
NETWORK

Fig. 44

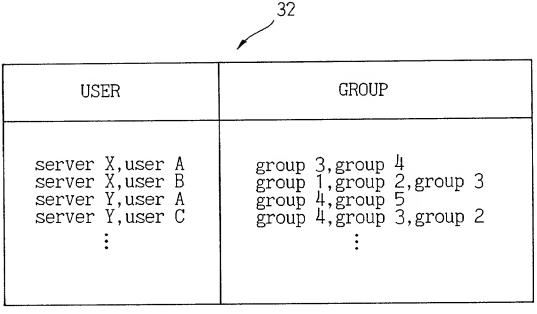

32
USER
GROUP
server X,user A
server X,user B
server Y,user A
server Y,user C
group 3,group 4
group 1,group 2,group 3
group 4,group 5
group 4,group 3,group 2

Fig.45

DATA HELD BY GROUP CERTIFICATE TEMPORARY STORING UNIT

52

GROUP CERTIFICATE			SESSION ID
NAME OF GROUP	VALID TERM INFORMATION time stamp	TEMPORARY PASSWORD temp	
server X.group 1	00/03/01 14:00	temp_a	4820100
server X.group 2	00/03/01 14:00	temp_b	4820100
server X.group 3	00/03/01 14:00	temp_c	4820100
server X.group 2	00/03/01 15:00	temp_d	2351121
server X.group 4	00/03/01 15:00	temp_e	2351121
⋮	⋮	⋮	⋮

Fig. 46

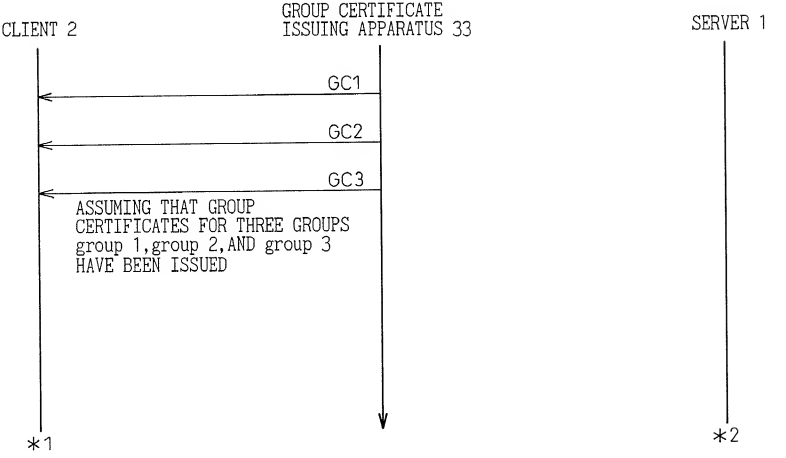

CLIENT 2
GROUP CERTIFICATE ISSUING APPARATUS 33
SERVER 1
GC1
GC2
GC3
ASSUMING THAT GROUP CERTIFICATES FOR THREE GROUPS group 1, group 2, AND group 3 HAVE BEEN ISSUED
*1
*2

Fig.47

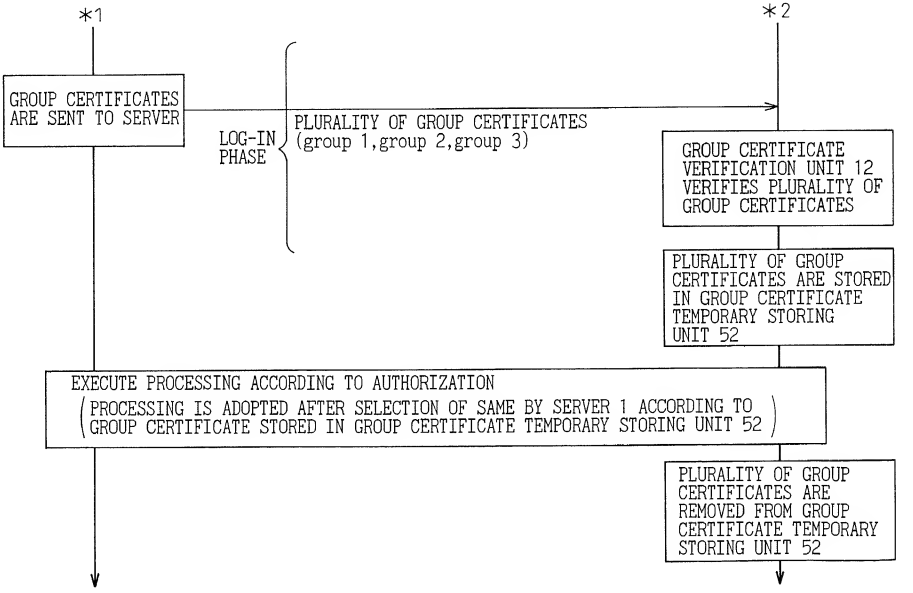

*1
*2
GROUP CERTIFICATES ARE SENT TO SERVER
LOG-IN PHASE
PLURALITY OF GROUP CERTIFICATES (group 1,group 2,group 3)
GROUP CERTIFICATE VERIFICATION UNIT 12 VERIFIES PLURALITY OF GROUP CERTIFICATES
PLURALITY OF GROUP CERTIFICATES ARE STORED IN GROUP CERTIFICATE TEMPORARY STORING UNIT 52
EXECUTE PROCESSING ACCORDING TO AUTHORIZATION
(PROCESSING IS ADOPTED AFTER SELECTION OF SAME BY SERVER 1 ACCORDING TO GROUP CERTIFICATE STORED IN GROUP CERTIFICATE TEMPORARY STORING UNIT 52)
PLURALITY OF GROUP CERTIFICATES ARE REMOVED FROM GROUP CERTIFICATE TEMPORARY STORING UNIT 52

Fig.48

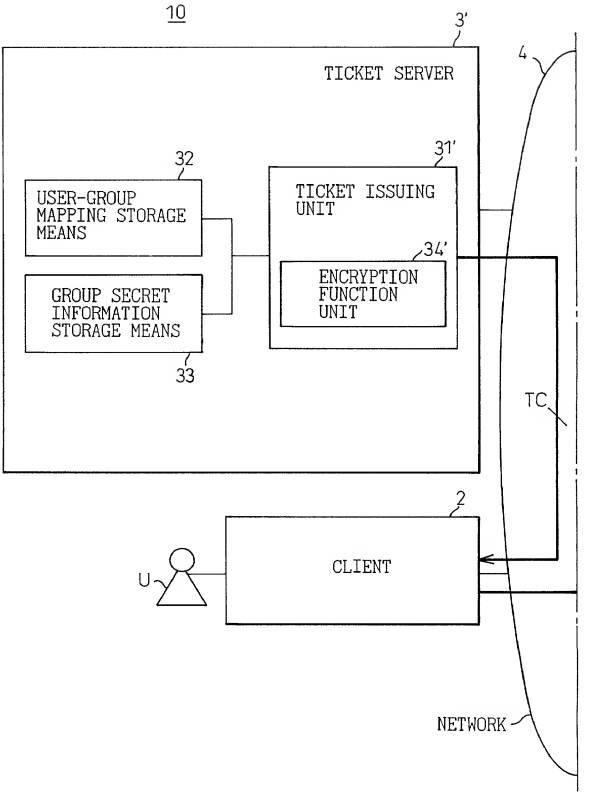
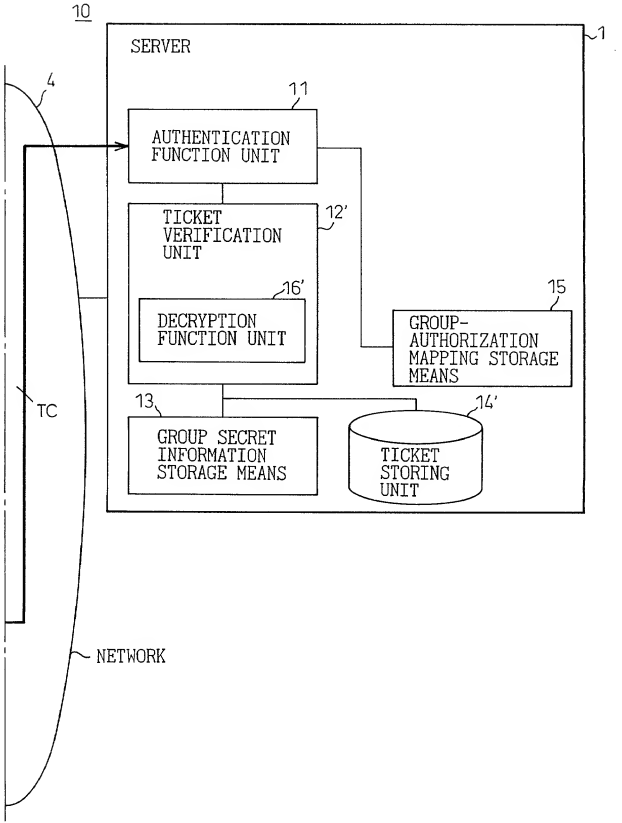

10
3'
TICKET SERVER
4
32
USER-GROUP MAPPING STORAGE MEANS
GROUP SECRET INFORMATION STORAGE MEANS
33
31'
TICKET ISSUING UNIT
34'
ENCRYPTION FUNCTION UNIT
TC
2
CLIENT
U
NETWORK

Fig. 49


10
SERVER
1
4
11
AUTHENTICATION FUNCTION UNIT
12'
TICKET VERIFICATION UNIT
16'
DECRYPTION FUNCTION UNIT
15
GROUP-AUTHORIZATION MAPPING STORAGE MEANS
TC
13
GROUP SECRET INFORMATION STORAGE MEANS
14'
TICKET STORING UNIT
NETWORK